Customer No. 24498
Attorney Docket No. PF020104
Office Action Date: 11/24/2009

REMARKS

This application has been reviewed in light of the Non Final Office Action dated November 24, 2009.

Claims 1–6 and 19-29 are pending in the application. Claims 7–18 have been withdrawn. Claim 6 has been amended to correct a typographical error. No new matter has been added.

ALLOWABLE SUBJECT MATTER

Applicant acknowledges with appreciation the Examiner's indication that claims 5-6, 20-21, 25-26 and 29 would be allowable is rewritten in independent form including all of the limitations of the base claims and any intervening claims.

§102/103 REJECTIONS

Claims 1–3, 19, 22–23 and 27-28 are rejected under 35 U.S.C. § 102(b) as being anticipated by, or in the alternative, under 35 U.S.C. 103(a) as obvious over U.S. Patent Publication No. 2002/0108058 to Iwamura (hereinafter "Iwamura").

To be anticipated under 35 U.S.C. 102, "the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present." *See* MPEP 706.02.

Iwamura is directed to an anti-theft system for electronic devices. Namely, Iwamura involves a system and method for implementing a software based security system for preventing the unauthorized disconnection of electronic equipment from a network. Iwamura's security software detects unauthorized disconnection of the

electronic equipment from the network and sends an alarm signal to the security station. The software determines whether devices are logged on to the network, then polls each logged on device. The logged on devices respond by sending an acknowledge signal which is sensed by the polling computer. In the event the acknowledge signal is not sensed, the polling computer sends an alarm signal to the security station.

Iwamura states that its network 19 comprises a LAN. The Examiner alleges that 'security station 15' in Iwamura comprises the 'watchdog device' of the present invention, and that the 'client computers 11, 12, 13' comprise the presently claimed 'electrical device.'

However, it is respectfully submitted that Iwamura fails to disclose or suggest at least identifying at least one watchdog device when the electrical device is connected to any network containing such a watchdog device, essentially as claimed in claims 1 and 19. Iwamura is completely silent with respect to any 'identifying **at least one watchdog device**' step being performed upon connection of a device to a network. In paragraph [0027], Iwamura states:

> "For example, a user connects the client computer 11 to the LAN 19 and the client security software is installed on the client computer 11. The user will run the client security software and log on with a password. The client security software on the client computer 11 sends a computer name identifying client computer 11 and the password to the local server 10. The security software of the local server 10 adds the computer name and the password to a polling list. ..."

Thus, upon connection of a computer 11 to the network 19 in Iwamura, the client computer automatically commences communication with the server 10. Any 'identifying' occurring in Iwamura simply involves **client** computer 11 sending a computer name identifying the **client computer** (NOT a watchdog device!), and a

password, to the server 10. This is NOT to be confused with identifying at least one **watchdog device** when an electrical device is connected to any network containing such a watchdog device. There is no need for such an 'identifying at least one watchdog device' feature in Iwamura, since normal log on messages and polling responses are broadcast over the LAN. Hence, identification of the local server or security station 15 is completely unnecessary in Iwamura.

Indeed, Iwamura teaches away from any step for identifying a watchdog device upon connection of an electrical device to a network. Paragraph [0029] explains that Iwamura provides a solution that is flexible and cost effective and adapts to changes in LAN configuration, as compared to hardware based systems that require physical installation at each connected computer. Assuming *arguendo*, that each computer in Iwamura had the 'identifying means' as presently claimed, then it would necessarily mean that each computer also had an up-to-date list of *all* the local servers that it could be connected to. For each change in LAN configuration, such a list would have to be updated. In particular, a new local server would have to be manually configured in the client computer. This can hardly be seen as a flexible and cost effective solution. Hence Iwamura teaches away from this feature.

Moreover, it is respectfully submitted that Iwamura fails to disclose or suggest at least the feature of **automatically disabling** the electrical device if the watchdog device identified does not correspond to the watchdog device for which the electrical device was configured, or if the network does not contain a watchdog device, essentially as claimed in claims 1, 19 and 27.

Applicant notes that it is readily apparent that Iwamura fails to explicitly disclose or teach any automatic disabling means. In particular, as previously argued, it is clear that Iwamura is silent with respect to an electrical device automatically disabling itself. Instead, the security of Iwamura simply involves generating an alarm signal which is sent to a security station wherein security personnel then respond to the alarm signal.

To reject a claim based on Section 103, the Examiner must articulate the following:

(1) a finding that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings;

(2) a finding that there was reasonable expectation of success; and

(3) whatever additional findings based on the *Graham* factual inquiries may be necessary, in view of the facts of the case under consideration, to explain a conclusion of obviousness.

The rationale to support a conclusion that the claim would have been obvious is that "a person of ordinary skill in the art would have been motivated to combine the prior art to achieve the claimed invention and that there would have been a rea sonable expectation of success." *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360, 80 USPQ2d 1641, 1645 (Fed. Cir. 2006). If any of these findings cannot be made, then this rationale cannot be used to support a conclusion that the claim would have been obvious to one of ordinary skill in the art. *See* MPEP 2143 (G).

The Examiner alleges that Iwamura teaches the claimed 'disabling means' and cites paragraph [0031], but Applicant respectfully disagrees. Iwamura teaches that when a client computer has gone AWOL, an alarm is sent to the security station, thereby alerting security personnel. The cited paragraph [0031] states "[S]ecurity personnel will then take appropriate action." According to the Examiner, such 'appropriate action' is taken to mean the disabling of the client computer.

However, even assuming *arguendo*, that the term 'appropriate action' can be taken to imply disabling a client computer, note that Iwamura states here that it is the security personnel who must perform an action to disable the client computer, not the client computer (i.e. electrical device) automatically operating to disable itself, essentially as claimed in claims 1 and 27. The Examiner alleges that it would have been obvious to a skilled person to modify Iwamura to do this. However, Applicant disagrees.

There is no teaching or suggestion in Iwamura for disabling the client computers 11, 12, 13. The Examiner, on page 3 of the Office Action, states that "[D]isable of an electrical device is one of the actions that the security personnel will act on based on the automatic alarm signal received from the server that client computer has already been automatically disconnected/disabled." However, there has been no explanation or demonstration provided by the Examiner as to what the motivation would be for one of skill in the art to do this. Namely, why would the security personnel disable the client computer? And how? For the Examiner to impute that the 'disabling' would be obvious here includes knowledge gleaned only from applicant's disclosure and thus constitutes impermissible hindsight reasoning. *See* MPEP 2145 (X)(A).

Indeed, it is emphasized that Iwamura is concerned with preventing **theft** of client computers. In order for security personnel to disable a client computer, as alleged by the Examiner, the security personnel would have to find it first, and if they find it then it's only reasonable to assume that they would desire to re-possess the computer, instead of disable it.

Applicant further points out that paragraph [0007] of Iwamura clearly states that it "is therefore desirable to provide an enhanced...system which detects the unauthorized removal of electronic hardware from a network." Thus, Iwamura repeatedly reiterates that it is simply a theft detection system. It is not a system that can remove the incentive to steal equipment by making sure that the equipment cannot work elsewhere, which is a feature advantageously provided by the present invention.

The statement beginning on page 3, line 17 of the Office Action (starting "Furthermore, paragraph 0029...") is unclear as far as relevance. What the Examiner refers to describes the problems of what Iwamura refers to as an inferior prior art hardware based solution (that, according to [0005] is undesirable). What's more, there is no support provided whatsoever for the Examiner's assertion that the "security card is configured to store secret information that monitor/detect unauthorized disconnection...[w]herein the secret information is a public identifier." Indeed, there is no mention in Iwamura of secret information. Further, the solutions based on security cards apparently come in three flavors: 1) ones that in essence are hardware solutions that are analogous to Iwamura's software solution, 2) ones that detect movement of the machine, and 3) ones that sense a current loop coupled to the machine. The first one does

not really differ from the Iwamura as discussed herein, while the second and third solutions require no secret information whatsoever.

Finally, as for the Examiner's argument in the last paragraph on page 3 of the Office Action, it is respectfully asserted that there *is* a structural difference between Iwamura and the present claimed invention. For example, claim 1 recites an automatic disabling means that, as already demonstrated, is not present or reasonably taught or suggested in Iwamura. Hence the claims *are* asserted to be patentably distinct in view of Iwamura.

For at least the above reasons, it is respectfully asserted that Iwamura does not disclose or suggest all of the elements of claims 1, 19 and 27. It is therefore believed that claims 1, 19 and 27 are patentable and nonobvious in view of Iwamura. Claims 2–3, 22–23 and 28 depend from claims 1, 19 and 27 respectively, and thus they include all of the limitations of their parent claims. As a result, it is also believed that claims 2–3, 22–23 and 28 are in condition for allowance. Reconsideration of the rejection is earnestly solicited.

Claims 4 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Iwamura in view of U.S. Patent No. 6,047,242 to Benson (hereinafter "Benson").

The rejection of claims 4 and 24 is based, in part, on the contention that Iwamura discloses or suggests the features of claims 1 and 19, from which such claims respectively depend. However, in view of the above amendments and arguments, it is clear that the combination of Banson with Iwamura is legally deficient, since, at the very least, as explained above, Iwamura fails to disclose or suggest the features of claims 1 and 19, from which claims 4 and 24 depend.

Furthermore, Benson is directed to copy protection for software, and as such has no bearing on anti-theft systems for physical devices. As Benson relates to a nonanalogous field of art, there would be no motivation or suggestion for one skilled in the art to combine Iwamura with Benson.

Reconsideration of the rejection is earnestly solicited.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to Applicant's representatives Deposit Account No. 07-0832.

Respectfully submitted,

Dated: 2/18/10

By: _____
Paul P. Kiel
Registration No.: 40,677

Mailing Address:

THOMSON LICENSING LLC
PATENT OPERATIONS
TWO INDEPENDENCE WAY
P.O. BOX 5312
PRINCETON, NJ 08543-5312